PLOS ONE

RESEARCH ARTICLE

Exploring new lengths for q-ary quantum MDS codes with larger distance

Xianmang He[1], **Jingli Wang**[1], **Chunfang Huang**[1], **Yindong Chen**[2,3]*

1 Ningbo University of Finance and Economics, Ningbo, China, **2** School of Mathematics and Computer Science, Shantou University, Shantou, China, **3** Key Laboratory of Intelligent Manufacturing Technology, Ministry of Education, Shantou University, Shantou, China

* ydchen@stu.edu.cn

Citation: He X, Wang J, Huang C, Chen Y (2025) Exploring new lengths for q-ary quantum MDS codes with larger distance. PLoS One 20(6): e0325027. https://doi.org/10.1371/journal.pone.0325027

Editor: Alemayehu Getahun Kumela, Universite Cote d'Azur, FRANCE

Received: October 29, 2024

Accepted: May 05, 2025

Published: June 5, 2025

Data availability statement: All relevant data are within the manuscript.

Funding: This study was financially supported by the Key Special Projects of the National Key

Abstract

In the past decade, the construction of quantum maximum distance separable codes (MDS for short) has been extensively studied. For the length $n = \frac{q^2-1}{m}$, where m is an integer that divides either $q+1$ or $q-1$, a complete set of results has been available. In this paper, we dedicate to a previously unexplored cases where the length $n = \frac{q^2-1}{m}$, subject to the conditions that m is neither a divisor of $q-1$ nor $q+1$. Ultimately, this problem can be summarized as exploring the necessary and sufficient conditions for the existence of pairs (m_1, m_2), where $m = \frac{m_1 \times m_2}{m_1+m_2-2}$ is an integer, with the additional requirement that the greatest common divisor (gcd) of m with both m_1 and m_2, $\gcd(m, m_1) > 1$ and $\gcd(m, m_2) > 1$, and $\gcd(m_1, m_2) = 2$. The quantum MDS codes presented herein are novel and exhibit distance parameters exceeding $\frac{q}{2}$.

1 Introduction

Quantum error-correction codes have been demonstrated as an encoding technique specifically engineered to safeguard quantum data against the effects of noise and interference. In quantum communication systems such as quantum key distribution (QKD), quantum MDS codes can be used to enhance the security and robustness of the key distribution process. They can help detect and correct errors that may occur during the transmission of quantum states used for key generation, ensuring the integrity of the shared secret key.

The construction of quantum error-correcting codes has been transformed into a finding for classical self-orthogonal codes over the fields $\mathbb{F}_2$ or $\mathbb{F}_4$ with respect to specific inner products, as referenced in [3]. This concept was later extended to the non-binary cases in [1,21]. Henceforth, the construction of quantum error-correcting codes has seen significant advancements following the realization of the interplay between quantum codes and classical codes. Let q be a prime power, and a q-ary quantum code is defined as K-dimensional subspace within the Hibert space $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$, which is capable of detecting quantum errors at most $d-1$. Let $k = \log_q K$, and we denote a q-ary quantum code as $[[n,k,d]]_q$. Similar to classical coding theory, one of the fundamental challenge in quantum coding theory is to develop quantum codes with desirable parameters. The inequality $2d \leq n - k + 2$ provides a bound on the distance achievable for a quantum code $[[n,k,d]]_q$ (as detailed in [17,18]). A quantum code attaining this bound is referred to as a quantum maximum-distance-separable

R&D Program of China in the form of an award (2022YFB3103100) received by XH. This study was also financially supported by the National Natural Science Foundation of China Special Project in the form of an award (J2324013) receibed by XH. This study was also financially supported by the Ningbo Education Science Planning Research Project in the form of an award (2024YGH040) received by XH. This study was also financially supported by the Yongjiang Talent Project of Ningbo in the form of an award (2024A-398-G) received by XH. This study was also financially supported by the 14th Five Year Plan Teaching Reform Project of Zhejiang Province in the form of an award (jg20220633) received by JW. This study was also financially supported by the Second Batch of Undergraduate Teaching Reform Projects During the 14th Five Year Plan of Zhejiang Province in the form of an award (JGBA2024612) received by JW. This study was also financially supported by the Key Research Platforms and Projects of Higher Education Institutions in Guangdong Province in the form of an award (2024ZDZX1021) received by YC. This study was also financially supported by the Basic and Applied Basic Research Foundation of Guangdong Province in the form of an award (2025A1515012156) received by YC. This study was also financially supported by the Science and Technology Planning Projects of Shantou, China in the form of an award (220516096491783) received by YC.

Competing interests: The authors have declared that no competing interests exist.

(MDS) code. Numerous classes of quantum MDS codes have been systematically constructed employing various approaches.

The Hermitian inner produce over $\mathbb{F}_{q^2}^n$ is defined as follows. $< u, v >_h = u_1 v_1^q + \cdots + u_n v_n^q$, where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ are vectors in $\mathbb{F}_{q^2}^n$. The approach outlined below represents a construction of q-ary quantum MDS codes from Hermitian self-orthogonal MDS codes over $\mathbb{F}_{q^2}^n$, which is one of the significant techniques presented in [1].

Theorem 1 (*Hermitian Construction*)**.** *Suppose that* $\mathbb{C}$ *is an* $[[n, k, n-k+1]]_{q^2}$ *MDS code over* $\mathbb{F}_{q^2}$*, and is orthogonal with respect to the Hermitian inner product. Then we can construct a q-ary quantum MDS code of parameters* $[[n, n-2k, k+1]]_q$.

1.1 Contributions and organization

The quantum MDS codes have several potential applications: one of the most important applications is in quantum error correction, and can be used to detect and correct errors in quantum information. By using quantum MDS codes, quantum operations can be performed in a way that is resilient to certain types of errors. This is essential for building large-scale and practical quantum computers that can run complex algorithms without being overwhelmed by errors.

Contributions. For length of the form $\frac{q^2-1}{m}$, where m is an integer such that m divides $q-1$ or m divides $q+1$, comprehensive results are available, as shown in Table 1. The notation $[a, b]$ represents the inclusive set of integers from a to b. However, in this paper, we concentrate on the case where m is not a divisor of either $q-1$ or $q+1$. Specifically, we consider pairs (m_1, m_2) such that $m = \frac{m_1 \cdot m_2}{m_1+m_2-2}$ is an integer and $\gcd(m_1, m_2) = 2$.

1. When m odd, $m|q-1$, it is clear that Hermitian self-orthogonal MDS codes can't be constructed with the length $n = \frac{q^2-1}{m}$. As illustrated in Corollary 1, our construction covers some cases.
2. We provide the necessary and sufficient conditions for the existence of pairs (m_1, m_2) that makes $m = \frac{m_1 \cdot m_2}{m_1+m_2-2}$ an integer.
3. Additionally, for any given integer $m = a_1 b_1$, Algorithms 1 and 2 help us determine several possible pairs (m_1, m_2) such that $m = \frac{m_1 \cdot m_2}{m_1+m_2-2}$ is an integer.

Organization. The rest part of this paper is structured as below. In Sect 2: Previous Known Results, we briefly review the previous known results about constructions for quantum MDS codes. In Sect 3: Preliminaries, we introduce the necessary preliminaries. Our main results are established in Sect 4: Constructions. The paper comes to an end in Sect 5: Conclusion.

2 Previous known results

The construction of quantum MDS codes has been a significant area of research since the pioneering work of Shor [23] and the subsequent generalizations by Calderbank, Rains, Shor,

Table 1. Quantum MDS code with Length $\frac{q^2-1}{m}$.

Length	Distance	References
$\frac{q^2-1}{m}$, $m\|q+1$, m even	$d \in [2, \frac{q-1}{2} + \frac{q+1}{m}]$	[24,25]
$\frac{q^2-1}{m}$, $m\|q+1$, m odd	$d \in [2, \frac{q-1}{2} + \frac{q+1}{2m}]$	[4,10,24]
$\frac{q^2-1}{m}$, $m\|q-1$, m even	$d \in [2, \frac{q+1}{2} + \frac{q-1}{m}]$	[4,10]

https://doi.org/10.1371/journal.pone.0325027.t001

and Sloane [3]. These works laid the foundation for constructing quantum codes using classical codes over finite fields. The central idea is to find classical self-orthogonal codes with certain properties and then convert them into quantum codes [1,21].

An important method for constructing quantum MDS codes is the Hermitian construction. This method involves finding classical codes that are self-orthogonal with respect to the Hermitian inner product. The Hermitian construction has been used to create quantum MDS codes with larger minimum distances than those achievable through Euclidean self-orthogonal codes. For example, Jin, Ling, Luo, and Xing have used classical Hermitian self-orthogonal MDS codes to construct quantum MDS codes [12,13]. Additionally, Kai and Zhu have developed new quantum MDS codes from negacyclic codes [15], and Zhang and Chen have introduced new quantum MDS codes with large minimum distances [4]. Xueying Shi, Qin Yue and Xiaomeng Zhu use the classical Hermitian self-orthogonal generalized Reed-Solomon codes to construct some new quantum MDS codes with minimum distance bigger than $\frac{q}{2}+1$ [22]. Reference [6] constructs six new classes of q-ary quantum MDS codes by using generalized Reed-Solomon (GRS) codes and Hermitian construction.

Generalized Reed-Solomon (GRS) codes have been particularly useful in constructing quantum MDS codes. GRS codes are a generalization of the classical Reed-Solomon codes and are known for their optimal error-correcting capabilities. By using GRS codes, several new classes of quantum MDS codes have been constructed with parameters that exceed the minimum distance of previously known codes. For example, Reference [20] constructs a new family of quantum MDS codes from classical generalized Reed-Solomon codes and derive the necessary and sufficient condition for the existence. Jin [14] presents a new construction of quantum MDS codes with minimum distance greater than $\frac{q}{2}+1$. The authors use Hermitian self-orthogonal codes to construct these new quantum MDS code. Reference [2] constructs quantum MDS codes with parameters $[[q^2+1, q^2+3-2d, d]]_q$ for all $d \leq q+1$, $d \neq q$. These codes are shown to exist by proving that there are classical generalised Reed-Solomon codes which contain their Hermitian dual.

Constacyclic codes over finite fields have been another rich source for constructing quantum MDS codes. These codes offer a flexible structure that can be tailored to achieve the MDS property. Kal et al. [16] generated several classes of quantum MDS codes based on constacyclic codes. Subsequently, Chen et al. [4] got four families of q-ary quantum MDS codes through MDS cyclic codes. Hu et al. [11] proposed a way to determine the maximum distance of $[[n,k,d]]_q$ quantum MDS codes from constant cyclic codes with the given n and q, and in the meanwhile presented a new class of quantum MDS codes derived from Hermitian dual-containing MDS constacyclic code. Kai and Zhu [15] construct two families of quantum MDS codes by leveraging negacyclic codes.

In recent years, a plenty of quantum MDS codes possessing favorable properties have been derived from classical error-correcting codes, including algebraic-geometric codes, BCH codes, and Reed-Muller codes, as detailed in References [5], [7], [14], [13], [12] etc. The underlying principle of constructing the Hermitian self-orthogonal codes hinges on the solvability in $\mathbb{F}_q$ of a system of homogenous equations over $\mathbb{F}_{q^2}$ [14]. By applying Hermitian self-orthogonal algebraic geometry codes to quantum codes, some good quantum codes were obtained [13]. Grassl et al. [9] constructed a class of q-ary quantum MDS codes with length $n = q^2 - 1$. La Guardia [19] constructed a class of quantum MDS codes utilizing MDS cyclic codes. By identifying polynomials rooted in appropriate trace functions, a novel family of linear codes was introduced, facilitating the construction of stabilizer quantum codes over several finite fields [8].

3 Preliminaries

In this section, we introduce a straightforward approach to constructing generator matrices that are crucial for the formation of Hermitian self-orthogonal MDS codes over the finite field $\mathbb{F}_{q^2}$ as detailed in Reference [10]. This approach not only recaptures the case where the code length $n = \frac{q^2-1}{m}$, but also paves the way for the development of a variety of new MDS quantum codes. We will proceed with two key lemmas that are fundamental to our construction. However, we choose to omit the proofs of these lemmas and instead, direct the interested reader to Reference [10] for a comprehensive explanations of the proofs.

Lemma 2. *Let θ be a primitive element within the multiplicative group of the finite field $\mathbb{F}_{q^2}^*$, and an integer $m|q^2-1$, then $\sum_{j=1}^{\frac{q^2-1}{m}} \theta^{jtm} = 0$ except the case that $t|\frac{q^2-1}{m}$.*

Lemma 3. *Let $v_0, \ldots, v_n$ be n non-zero elements in the multiplicative group $\mathbb{F}_{q^2}^*$. Let $gl = (g_{1l}, \ldots, g_{nl})$ for $l = 1, \ldots, k$ be k linear independent rows in $\mathbb{F}_{q^2}^n$ such that $\sum_{j=1}^{n} v_j g_{jl_1} g_{jl_2}^q = 0$ for any two indices l_1 and l_2 in the set {1, …, k} (where $l_1 = l_2$ is allowed). Consequently, we can construct a Hermitian self-orthogonal $[n,k]_{q^2}$ code produced by these k rows.*

With Lemmas 2 and 3, given m, q, and $m|q^2-1$, for any fixed positive integer k, a linear error codes of length $\frac{q^2-1}{m}$ over $\mathbb{F}_{q^2}^n$ can be defined as follows:

$$\mathbb{C} = \Big\{\big(\theta^m f(\theta^m), \theta^{2m} f(\theta^{2m}), \ldots, \theta^{jm} f(\theta^{jm}), \ldots, \theta^{(\frac{q^2-1}{m}-1)m} f(\theta^{(\frac{q^2-1}{m}-1)m}), f(1)\big) : f \in \mathbb{F}_{q^2}[x], \deg(f) \le k-1\Big\}$$

It is evident that $\mathbb{C}$ is an MDS code with the parameters $[n = \frac{q^2-1}{m}, k, n-k+1]$ over $\mathbb{F}_{q^2}$. Essentially, this code is an evaluation code at the points $\theta^m, \theta^{2m}, \ldots, \theta^{(\frac{q^2-1}{m}-1)m}, 1$.

The Hermitian inner product of any two codewords (associated with two polynomials f and g) is $\sum_{j=1}^{\frac{q^2-1}{m}} \theta^{jm+jqm} f g^q(\theta^{jm})$. Thus, if the sum $\sum_{j=1}^{\frac{q^2-1}{m}} \theta^{jm(1+q+t_1+t_2q)} = 0$, where $\forall t_1, t_2 \in [0, k-1]$, then $\mathbb{C}$ is a Hermitian self-orthogonal MDS code.

4 Constructions

This section focuses on the construction of novel quantum MDS codes with a length of $\frac{q^2-1}{m}$, where $m \nmid q-1$ and $m \nmid q+1$, pairs (m_1, m_2) with $m = \frac{m_1 \cdot m_2}{m_1+m_2-2}$, $\gcd(m_1, m_2) = 2$, and q represents an odd prime power.

Let m_1, m_2 be two even integers. $m_1|q-1$, $m_2|q+1$. According to Lemma 3.1 in [10], we have the following identity when $0 \le t_1, t_2 \le \frac{q-1}{2} + \frac{q-1}{m_1} - 1$.

$$\sum_{j=1}^{\frac{q^2-1}{m_1}} \theta^{jm_1(t_1+t_2q)} \cdot \theta^{j\frac{m_1(q+1)}{2}} = 0.$$

According to Theorem 1 from Reference [25], the subsequent identity is established when $0 \le t_1, t_2 \le \frac{q-1}{2} + \frac{q+1}{m_2} - 2$:

$$\sum_{j=1}^{\frac{q^2-1}{m_2}} \theta^{jm_2(t_1+t_2q)} \cdot \theta^{jm_2(q+1)} = 0.$$

Table 2. New Quantum MDS code with $n = \frac{q-1}{k} \cdot (q+1)$.

(m_1, m_2)	q	m	Distance d
(8,6)	17	4	[2,11]
(8,6)	41	4	[2,27]
(10,8)	71	5	[2,44]
(12,10)	49	6	[2,29]
(14,12)	71	7	[2,31]
(16,14)	97	8	[2,56]
(18,16)	127	9	[2,71]

https://doi.org/10.1371/journal.pone.0325027.t002

By summing the two identities, we derive the following new identities:

$$\sum_{j=1}^{\frac{q^2-1}{m_2}} \theta^{jm_2(t_1+t_2q)} \cdot \theta^{jm_2(q+1)} + H\Big(\sum_{j=1}^{\frac{q^2-1}{m_1}} \theta^{jm_1(t_1+t_2q)} \cdot \theta^{j\frac{m_1(q+1)}{2}}\Big) = 0.$$

Here, H can be any nonzero element in $\mathbb{F}_q^*$, and the common position t_1, t_2 are in the range $0 \le t_1, t_2 \le \frac{q-1}{2} + \min\{\frac{q+1}{m_2} - 2, \frac{q-1}{m_1} - 1\}$.

Let M be the set $\{\theta^{jm_1} : j = 1, \dots, \frac{q^2-1}{m_1}\} \cup \{\theta^{jm_2} : j = 1, \dots, \frac{q^2-1}{m_2}\}$, and the code is the set $\{(f(x))_{x\in M} : 0 \le \deg(f) \le \frac{q-1}{2} + \min\{\frac{q+1}{2m_2} - 2, \frac{q-1}{m_1} - 1\}$.

Theorem 4. [25] *Let q be an odd prime power, m_1,m_2 be two even integers. $m_1 | q-1$, $m_2 | q+1$, then we construct a q-ary quantum MDS code with the following parameters:*

1. *length n: $\frac{q^2-1}{m_1} + \frac{q^2-1}{m_2} - \frac{q^2-1}{\mathrm{lcm}(m_1,m_2)}$, where $\mathrm{lcm}(m_1, m_2)$ denotes the least common multiple of m_1, m_2.*
2. *minimum distance d: $2 \le d \le \frac{q-1}{2} + \min\{\frac{q+1}{m_1}, \frac{q-1}{m_2}\}$.*

In Theorem 4, by carefully selecting specific parameters for the pair (m_1, m_2), we can derive a novel class of quantum codes that exhibit highly beneficial properties, as demonstrated in Corollary 1.

Corollary 1. *With the notation defined as above, $m_1 = 2k$ is an even divisor of $q-1$, $m_2 = 2k-2 \ge 3$ is an even divisor of $q+1$, then we can construct an q-ary quantum MDS code with the parameters:*

1. *length n: $\frac{q^2-1}{k} = \frac{q-1}{k} \cdot (q+1)$,*
2. *minimum distance d: $d \in [2, \frac{q-1}{2} + \frac{q+1}{2k-2}]$.*

Remark 1. When q odd, $k | q-1$, it is clear that Hermitian self-orthogonal MDS codes can't be constructed by the generator matrices over the finite field $\mathbb{F}_{q^2}$ as detailed in [10]. However, this case is partially covered by Corollary 1.

Theorem 4 provides the theoretical result of the construction, but it must be ensured that $m = \frac{m_1 m_2}{m_1+m_2-\gcd(m_1,m_2)}$ is an integer. This allows us to choose certain values pair (m_1, m_2) such that $m \nmid q-1, m \nmid q+1$, but $\gcd(m, q-1) > 1, \gcd(m, q+1) > 1$. This case has not been systematically discussed and studied.

Lemma 5. *Let m_1, m_2 be two even integers, and* $\gcd(m_1, m_2) = 2$. *If* $m = \frac{m_1 \times m_2}{m_1 + m_2 - 2}$ *is an integer,* $\gcd(m_1, m) > 1, \gcd(m_2, m) > 1$, *then, at least one of $m_1 and m_2$ has a factorization with at least three prime factors.*

Proof: The proof can be accomplished by introducing the method of proof by contradiction. Without loss of generality, we can assume that $m_1 = 2a_1$, $m_2 = 2b_1$, both $a_1 and b_1$ are primes, otherwise, either $m_1 or m_2$ has three factors. Hence, we have $m = \frac{2a_1 \cdot 2b_1}{2a_1 + 2b_1 - 2}$. Note that $m = 4, 2a_1 or 2b_1$, then $a_1 b_1 = a_1 + b_1 - 1, b_1 = a_1 + b_1 - 1 or a_1 = a_1 + b_1 - 1$, which is completely impossible. Therefore, $m_1 or m_2$ has at least three prime factors. □

Remark 2. Consider that $\gcd(m_1, m_2) = 2$, m_1, m_2 even, therefore, the factorization of m_1 or m_2, one with one factor 2 and the other can have multiple factors 2. We can assume that $m_1 = 2a_1 a_2$, a_1, a_2 odd, $m_2 = 2b_1 b_2$, b_1,b_2 can be odd or even, otherwise, $\gcd(m_1, m_2) \neq 2$.

In the following text, assume that $m_1 = 2a_1 a_2$, $a_1, a_2 \geq 3$ odd, $m_2 = 2b_1 b_2$, $b_1, b_2 \geq 2$, $\gcd(a_1 a_2, b_1 b_2) = 2$, $m = \frac{2a_1 a_2 \cdot 2b_1 b_2}{2a_1 a_2 + 2b_1 b_2 - 2}$.

Theorem 6. *The necessary and sufficient conditions for the existence of (m_1, m_2) pairs is $m_1 or m_2$ has at least three prime factors. Here, $m = \frac{m_1 \times m_2}{m_1 + m_2 - 2}$ is an integer and* $\gcd(m, m_1) > 1$ *and* $\gcd(m, m_2) > 1$.

Proof: From Lemma 5, we know that $m_1 or m_2$ has at least three prime factors. Next, we just need to prove that the pairs (m_1, m_2) always exists as long as $m_1 = 2a_1 a_2, m_2 = 2b_1 b_2$.

Let $m = \frac{2a_1 a_2 \cdot 2b_1 b_2}{2a_1 a_2 + 2b_1 b_2 - 2} = 2a_1 b_1$, then we have $2a_1 a_2 + 2b_1 b_2 - 2 = 2a_2 b_2$, then $b_2(a_2 - b_1) = a_1 a_2 - 1$.

With the assumption that a_1, a_2 are odd, therefore, $a_1 a_2 - 1$ can be factorised into $p_1 p_2$, that is, $b_2(a_2 - b_1) = a_1 a_2 - 1 = p_1 p_2$. Hence, let $b_2 = p_1, a_2 - b_1 = p_2$ or $b_2 = p_2, a_2 - b_1 = p_1$ to make the equation holds.

Now, we need to prove that $a_2 - p_1 \geq 2$. From the equation $a_1 a_2 = p_1 p_2 + 1$, and a_1, a_2 odd, then we have $a_2(a_1 - 2) \geq p_1^2 + 1$. $a_2^2 - 2a_2 - p_1^2 - 1 \geq 0$, $(a_2 - 1)^2 \geq p_1^2 + 2$, $a_2 - 1 \geq \sqrt{p_1^2 + 2} > p_1 + \sqrt{2}$. $a_2 - p_1 > 1 + \sqrt{2}$. Consider that a_2, p_1 are integers, therefore, $a_2 \geq p_1 + 2$.

The conclusion holds. □

Remark 3. Theorem 6 provides an existence case, and other cases can be similarly proved. For example, when $m_1 = 2p$, p odd. Even if p a prime, we can also prove its existence. Let $m_2 = 2b_1 b_2$, $b_1, b_2 \geq 2$ integers. Similarly, let $m = 2b_1$, then we have $pb_2 = p + b_1 b_2 - 1$, $(p - b_1)b_2 = p - 1$. Hence, let $b_1 = \frac{p+1}{2}$, $b_2 = 2$ to make the equation holds. We treat this case in the following Algorithm 1.

Algorithm 1. Algorithm for determining parameters m_1, m_2.

Input: input parameters $m = 2 \cdot b_1$
Output: m_1, m_2
$p = 2 \cdot b_1 - 1$;
$b_2 = 2$;
$m_1 = 2 \cdot p = 4 \cdot b_1 - 2$;
$m_2 = 4 \cdot b_1$;
return

Remark 4. Theorem 6 demonstrates that given an arbitrary m_1, m_2 can always be found such that $\frac{m_1 m_2}{m_1 + m_2 - 2}$ is an integer. Similarly, given m_2, m_1 can also be found such that $\frac{m_1 m_2}{m_1 + m_2 - 2}$ is an integer. Considering that this proof is identical, we omit here. The prerequisite for this is that m_1 or m_2 has at least three prime factors.

Algorithm to choose the parameters m_1, m_2

Theorem 6 only tells us the existence of the pair (m_1, m_2), we need to fully determine the value of a pair (m_1, m_2). Given any integer $m = a_1 b_1$, Algorithm 2 can help us determine several possible pairs (m_1, m_2).

According to the proof process of Theorem 6, the algorithm run through the variable p_1, which varies from 1 to $a_1 b_1 - 1$ or larger, which can be used to determine the pair (m_1, m_2). From Corollary 2, $p_2 \in Z$ always exists.

Corollary 2. *Given two integer $a_1 \geq 2$ odd and $b_1 \geq 1$, $m = 2 \cdot a_1 \cdot b_1$, there exists a pair (p_1, p_2) that makes $m = \frac{m_1 m_2}{m_1 + m_2 - 2} \in Z$, Here, $p_2 = \frac{a_1(b_1+p_1)-1}{p_1}$, $m_1 = 2a_1(b_1 + p_1), m_2 = 2b_1 p_2$.*

Proof: Assume that $p_1 = a_1 b_1 - 1$, then $p_2 = \frac{a_1(b_1+p_1)-1}{p_1} = 1 + a_1 \geq 2 \in Z$. The corollary holds. □

Algorithm 2. Algorithm for determining parameters m_1, m_2.

Input: input parameters $m = 2 \cdot a_1 \cdot b_1, a_1$ odd
Output: m_1, m_2
for $p_1 = 1 to \infty$ **do**
  if $p_1 | (a_1 \cdot (p_1 + b_1) - 1)$ **then**
    $p_2 = \frac{a_1 \cdot (p_1 + b_1) - 1}{p_1}$;
    $b_2 = p_2$;
    $a_2 = b_1 + p_1$;
    $m_1 = 2 \cdot a_1 \cdot a_2$;
    $m_2 = 2 \cdot b_1 \cdot b_2$;
  else
    $p_1 += 1$;
  end
end
return

With Algorithm 1, we can get the value of pairs (m_1, m_2). Let's make some examples to illustrate this.

Example 1. Let $m = 2a_1 b_1 = 2 \cdot 3 \cdot 4$, $p_1 = a_1 \cdot b_1 - 1 = 11$, then $m_1 = 2 \cdot 3 \cdot (4 + 11) = 90, m_2 = 2 \cdot 4 \cdot \frac{a_1 \cdot (p_1 + b_1) - 1}{p_1} = 32$. Let $p_1 = 1$ also can give a pair of $m = 24$, $b_2 = \frac{a_1 \cdot (p_1 + b_1) - 1}{p_1} = 7$, $m_1 = 30$, $m_2 = 112$.

Example 2. Let $m = 2a_1 b_1 = 2 \cdot 3 \cdot 5$, $p_1 = 1, b_2 = 17$, then $m_1 = 36, m_2 = 170$. Case $p = 2$ can also give a pair (m_1, m_2) with $m = 30$, $m_1 = 42, m_2 = 100$. Let $p_1 = 7$, $m_1 = 72, m_2 = 50$. If $p = 14$, $m_1 = 113, m_2 = 40$.

Example 3. Let $m = 2a_1 b_1 = 2 \cdot 5 \cdot 4$, $p = 1$, then $m_1 = 50, m_2 = 192$. Let $p_1 = 19$, then $m_1 = 230, m_2 = 48$.

Now, we need to determine the q that makes $m = a_1 b_1, m_1 | q - 1, m_2 | q + 1, m \nmid q - 1, m \nmid q + 1$. Consider that $\gcd(m_1, m_2) = 2$, then there exists two integers l_0, k_0 fulfilling $l_0 m_1 + 2 = k_0 m_2$. Set $q = m_1 m_2 t + l_0 m_1 + 1$, or $q = m_1 m_2 t + k_0 m_2 - 1$ and it is easy to verify that $m_1 | q - 1, m_2 | q + 1$. Table 3 gives some examples of new quantum MDS codes, with the length $n = \frac{q^2 - 1}{m}$, but $m \nmid q - 1, m \nmid q + 1$.

Remark 5. The integer 2 plays a special role throughout the entire paper, including $\gcd(m_1, m_2) = 2$, $m = \frac{m_1 \cdot m_2}{m_1 + m_2 - 2}$. The reason for doing this is to consider the existence of q, which only exists when $\gcd(m_1, m_2) = 1$ or 2, and satisfies $m_1 | q - 1$, $m_2 | q + 1$ in the meanwhile.

Table 3. New Quantum MDS code with $n = \frac{q^2-1}{m}, m \nmid q-1, m \nmid q+1$.

(m_1, m_2)	q	m	Distance d
(30,112)	449	24	228
(90,32)	449	24	229
(18,32)	127	12	66
(42,16)	127	12	66
(50,32)	449	20	233
(30,56)	449	20	232
(110,24)	769	20	391
(40,114)	1481	30	752

https://doi.org/10.1371/journal.pone.0325027.t003

5 Conclusion

In this paper, we have conducted a investigation of the case where the length is given by $n = \frac{q^2-1}{m}$, under the conditions that $m \nmid q-1, m \nmid q+1$, $m = \frac{m_1 m_2}{m_1+m_2-2}$, where $m_1 and m_2$ are both even, and $\gcd(m_1, m_2) = 2$. We have derived the necessary and sufficient conditions for the existence of such pairs (m_1, m_2). Additionally, for a specified value of m, we design Algorithms 1 and 2 to determine the pair (m_1, m_2). With these insights, it is now a straightforward task to construct a new class of quantum MDS codes.

Despite the numerous methods have been proposed to construct quantum MDS codes, in fact, the code length n is still sparse for $q \le n \le q^2$. In most cases, codes have not been constructed because the majority of the constructed results are concentrated in the case of $n = \frac{q^2-1}{m}$. Our future work is to develop a general method that is not limited to the case of length $n = \frac{q^2-1}{m}$.

Author contributions

Funding acquisition: Xianmang He, Yindong Chen.

Investigation: Xianmang He, Yindong Chen.

Methodology: Xianmang He.

Validation: Xianmang He, Jingli Wang, Chunfang Huang, Yindong Chen.

Writing – original draft: Xianmang He.

Writing – review & editing: Xianmang He, Jingli Wang, Chunfang Huang, Yindong Chen.

References

1. Ashikhmin A, Knill E. Nonbinary quantum stabilizer codes. IEEE Trans Inform Theory. 2001;47(7):3065–72. https://doi.org/10.1109/18.959288
2. Ball S. Some constructions of quantum MDS codes. Berlin: Springer; 2021.
3. Calderbank A, Rains E, Shor P, Sloane N. Quantum error correction via codes over GF(4). IEEE Trans Inf Theory. 1998;44(4):1369–87.
4. Chen B, Ling S, Zhang G. Application of constacyclic codes to quantum MDS codes. IEEE Trans Inform Theory. 2015;61(3):1474–84. https://doi.org/10.1109/tit.2015.2388576
5. Cohen G, Encheva S, Litsyn S. On binary constructions of quantum codes. IEEE Trans Inform Theory. 1999;45(7):2495–8. https://doi.org/10.1109/18.796389
6. Fang W, Fu F-W. Some new constructions of quantum MDS codes. IEEE Trans Inform Theory. 2019;65(12):7840–7. https://doi.org/10.1109/tit.2019.2939114
7. Feng K. Quantum codes $[[6,2,3]]_p and [[7,3,3]]_p (p3)$ exist. IEEE Trans Inf Theory. 2002;48(8):2384–91.

8. Galindo C, Hernando F, Ruano D. Classical and quantum evaluation codes at the trace roots. IEEE Trans Inform Theory. 2019;65(4):2593–602. https://doi.org/10.1109/tit.2018.2868442
9. Grassl M, Rötteler M. Quantum MDS codes over small fields. In: 2015 IEEE international symposium on information theory (ISIT). 2015. p. 1104–1108.
10. He X, Xu L, Chen H. New q-ary quantum MDS codes with distances bigger than $\frac{q}{2}$. Quantum Inf Process. 2016;15(7):2745–58. https://doi.org/10.1007/s11128-016-1311-2
11. Hu L, Yue Q, He X. Quantum MDS codes from BCH constacyclic codes. Quantum Inf Process. 2018;17(12). https://doi.org/10.1007/s11128-018-2049-9
12. Jin L, Ling S, Luo J, Xing C. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans Inform Theory. 2010;56(9):4735–40. https://doi.org/10.1109/tit.2010.2054174
13. Jin L, Xing C. Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes. IEEE Trans Inform Theory. 2012;58(8):5484–9. https://doi.org/10.1109/tit.2011.2177066
14. Jin L, Xing C. A Construction of new quantum MDS codes. IEEE Trans Inform Theory. 2014;60(5):2921–5. https://doi.org/10.1109/tit.2014.2299800
15. Kai X, Zhu S. New quantum MDS codes from negacyclic codes. IEEE Trans Inform Theory. 2013;59(2):1193–7. https://doi.org/10.1109/tit.2012.2220519
16. Kai X, Zhu S, Li P. Constacyclic codes and some new quantum MDS codes. IEEE Trans Inform Theory. 2014;60(4):2080–6. https://doi.org/10.1109/tit.2014.2308180
17. Ketkar A, Klappenecker A, Kumar S, Sarvepalli PK. Nonbinary stabilizer codes over finite fields. IEEE Trans Inform Theory. 2006;52(11):4892–914. https://doi.org/10.1109/tit.2006.883612
18. Knill E, Laflamme R. Theory of quantum error-correcting codes. Phys Rev A. 1997;55(2):900–11.
19. La Guardia GG. New quantum MDS codes. IEEE Trans Inform Theory. 2011;57(8):5551–4. https://doi.org/10.1109/tit.2011.2159039
20. Li Z, Xing L-J. Quantum generalized Reed-Solomon codes. Acta Phys Sin. 2008;57(1):28. https://doi.org/10.7498/aps.57.28
21. Rains EM. Nonbinary quantum codes. IEEE Trans Inform Theory. 1999;45(6):1827–32. https://doi.org/10.1109/18.782103
22. Shi X, Yue Q, Zhu X. Construction of some new quantum MDS codes. Finite Fields Their Appl. 2017;46:347–62. https://doi.org/10.1016/j.ffa.2017.04.002
23. Shor P. Scheme for reducing decoherence in quantum computer memory. Phys Rev A. 1995;52(4):R2493–6. https://doi.org/10.1103/physreva.52.r2493 PMID: 9912632
24. Wang L, Zhu S. New quantum MDS codes derived from constacyclic codes. Quantum Inf Process. 2015;14(3):881–9. https://doi.org/10.1007/s11128-014-0903-y
25. He X. Constructing new q-ary quantum MDS codes with distances bigger than $q/2$ from generator matrices. QIC. 2018;18(3 & 4):223–30. https://doi.org/10.26421/qic18.3-4-3